2016 Policy Review

Doc. #	Policy Information
PO1000	**Policy and Procedure Development** **Summary**: This policy establishes the form and content criteria for the West Virginia Office of Technology (WVOT) regarding information technology (IT) policy and procedure development, maintenance, and distribution to agencies within the State of West Virginia Executive Branch. **Edits**: Policy reviewed. No edits made.
PO1001	**Information Security Policy** **Summary**: The intent of this policy is to explain the range of acceptable and unacceptable uses of State-provided information technology (IT) resources **Edits**: Policy reviewed. No edits made.
PO1002	**Acceptable Use of State-Provided Wireless Devices** **Summary:** This policy establishes a framework for the procurement, possession, and appropriate use of West Virginia state-owned and/or paid wireless communication equipment and/or services. In addition, all rules regarding the acceptable use of IT resources within State agencies apply to the utilization of portable devices. **Edits**: Policy reviewed. No edits made.
PO1005	**Email Use Standards** **Summary**: This policy establishes and communicates the acceptable use of, access to, and disclosure of the State-provided e-mail system. **Edits**: Policy reviewed. No edits made.
PO1006	**Data Classification** **Summary**: This policy presents the framework through which all State of West Virginia (State) government agencies, employees, vendors, and business associates, specifically those in the Executive Branch, must classify their data and systems, as they relate to (1) data sensitivity; and (2) data and system criticality **Edits**: Renamed Classification Categories. "Extremely Sensitive Data" and "Very Sensitive Data" now combine to form the "Restricted" category. "Unrestricted Data" now named "Public Data"
PO1008	**Auditing Program** **Summary**: The West Virginia Office of Technology (WVOT) will maintain an objective and internally independent Information Security Audit Program. This program will serve the Executive Branch by examining, evaluating, and reporting on information technology (IT) applications, related systems, operations, processes, and practices to provide reasonable assurance security controls. **Last Edits**: Reviewed policy. Minor text changes to clarify language in section 3.16
PO1010	**Acceptable Use of State-Provided Instant Messaging** **Summary:** This policy Outline the applicable rules applied when using the State-provided system. **Edits:** Policy reviewed. No edits made.
PO1011	**Media Protection** **Summary**: This policy defines standards, procedures, and restrictions for Executive Branch employees who use authorized removable media to connect to any device attached to a WVOT-supported network, in order to store, back-up, relocate, or otherwise access enterprise data in a safe, secure manner. **Edits**: Policy reviewed. No edits made.

Doc. #	Policy Information
PO1012	**Contractor Management** **Summary**: This policy provides standard methodology to help manage the activities surrounding the engagement and termination of contractor services in the IT environment for the State. **Edits**: Policy reviewed. No edits made.
PO1013	**Data Backup and Retention** **Summary:** This policy outlines data backup requirements for the West Virginia Office of Technology (WVOT) to ensure availability of critical data and systems within Executive Branch agencies. **Edits:** Policy reviewed. No edits made.
PO1014	**Anti-Virus / Malicious Software** **Summary**: This policy describes prescribes the measures required to counter computer viruses, malicious code, and other malware. It identifies responsibilities in protecting the State network against malicious software. **Edits**: Policy reviewed. No edits made.
PO1015	**Change and Configuration Management** **Summary**: The purpose of Enterprise Change Management is to standardize the identification, evaluation, planning, coordination, communication and implementation of changes to the State computing environment in such a way as to minimize any potential disruption to the user community, to ensure that all impacted users and support groups are making necessary accommodations to the change(s), and to increase the value of Information Resources. **Edits**: Policy reviewed. No edits made.
PO1017	**Use of Social Media** **Summary**: Social media/social networking provides an additional method for communicating with West Virginia State Citizens; State agencies; agencies outside the State; business partners; and current, future, and former employees. It is an optional model for interaction that can assist employees in building stronger, more successful citizen and agency business relationships. This document provides policy for the professional use of internal and external social media (i.e. Facebook, Twitter, YouTube, Flickr, etc.) at State of West Virginia Executive agencies. **Edits**: Policy reviewed. No edits made.
PO1018	**Network Violation Reporting** **Summary**: The purpose of this policy is to outline the courses of action prescribed for both the West Virginia Office of Technology (WVOT) and Executive Branch agencies when network violations are detected on the State network. **Edits**: Policy reviewed. No edits made.
PO1019	**Wireless Access Point** Summary: This document prescribes how wireless technologies will be deployed, administered, and supported to assure that State of West Virginia employees, guests, and contractors have access to a reliable, robust, and integrated wireless network, and to increase the security of the wireless network to the fullest extent possible. **Edits:** Policy reviewed. No edits made.

Doc. #	Policy Information
PO1021	**Account Management** **Summary**: This policy outlines the standards for creating, issuing, removing, monitoring, and managing employee accounts. **Edits**: Added section 3.12 All temporary accounts must be designated as such, so users of those accounts cannot be mistaken for full-time state employees. 3.15.1 Where technically or administratively feasible, agencies may require Agency Identifiers in an email address account. An Agency Identifier is a 3-5 letter acronym representing the Agency's name. 3.15.2 Agencies may request an Identifier added to email addresses, in a format approved by WVOT, when: 3.15.2.1 Employees transfer OUT of the requesting Agency to the employment of another agency within West Virginia state government; 3.15.2.2 Employees transfer IN to the requesting Agency from the employment of another agency within West Virginia state government; 3.15.2.3 A new employee email account is created; or 3.15.2.4 In order to standardize all agency email accounts.
PO1022	**Internet Use** **Summary**: The intent of this policy is to explain the range of acceptable and unacceptable uses of State-provided internet access and is not necessarily all-inclusive. Questions about specific internet uses which are not detailed in this policy should be directed to an agency supervisor or manager. **Edits**: The term "sexually explicit" was replaced with "sexual in nature."
PO1025	**Accreditation and Certification** **Summary**: This policy is outlines how the West Virginia Office of Technology (WVOT) validates the security readiness for devices, systems, application and system software, and other technology prior to deployment into a production status. **Edits**: Policy reviewed. No edits made.
PO1026	**WVOT Monitoring Policy** **Summary**: The purpose of this document is to outline the West Virginia Office of Technology (WVOT) policy regarding the monitoring and logging of network traffic that traverses the WVOT Backbone. The goal of monitoring is to maintain the integrity and security of the State's network infrastructure and information assets. Any inspection of electronic data packets, and any action performed following such inspection, will be governed by all applicable federal and state statutes and by WVOT policies and procedures. **Edits**: Policy reviewed. No edits made.
PO1033	**Cloud Services** **Summary:** This document is intended to provide guidance to agencies and employees about the appropriate use of state-approved cloud service, WVOT's Microsoft One Drive for Business ("One Drive"). This policy contains risk factors all agency leaders and staff must review before using the cloud service. When using One Drive, information is stored remotely on servers owned by Microsoft and located in the continental United States. **Edits**: Policy reviewed. No edits made.
PR1001	**Technical Investigations** **Summary**: The purpose of this Procedure is to specify the process for State agencies when requesting an investigation into any State employee's technology-based activity. This procedure should not be construed to convey any expectation of privacy. **Edits**: Policy reviewed. No edits made.